АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНЖЕНЕРНЫХ НАУК

МАТЕМАТИЧЕСКИЕ АСПЕКТЫ БИТКОИНА И ЕГО СОЦИАЛЬНЫЕ И ЭКОНОМИЧЕСКИЕ ОСОБЕННОСТИ

Выонг Монг Хунг

Научный руководитель: Бурнашов Алексей Владимирович, к.ф.-м.н., ассистент ТПУ

Национальный исследовательский Томский политехнический университет

Как определить биткоин (bitcoin, btc, бтк, биткойн) простыми словами? Это новое поколение децентрализованной цифровой валюты (или еще говорят криптовалюты), созданной и работающей только в сети интернет. Таким образом, её никто не контролирует, эмиссия (выпуск новых монет) валюты происходит посредством работы миллионов компьютеров по всему миру с использованием программы для вычисления математических алгоритмов. Именно в этом заключается суть биткоина.

Децентрализованная валюта – это валюта, основной характеристикой которой является отсутствие какого-либо надзорного финансового регулятора, например, Центрального Банка Российской Федерации или Федеральной Резервной Системы США.

Но кто же печатает биткоины? Никто! Эта валюта не печатается центральным банком и не работает по его правилам. Банки могут выпустить сколько угодно денег, чтобы покрыть государственный долг, тем самым обесценивая свою валюту. Напротив, эмиссия биткоинов возможна только в цифровом виде, и любой желающий может начать добывать, или, как говорят, майнить биткоины в любое время. Майнинг биткоинов происходит посредством использования вычислительных мощностей компьютера в распределённой сети (рис. 1).

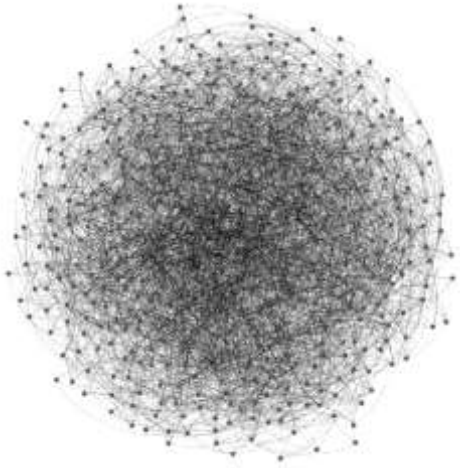

Рис. 1. Визуальное отображение децентрализованной сети биткоин.

Чем обеспечен биткоин? Национальные валюты раньше обеспечивались золотом или серебром, сейчас — ВВП. Теоретически вы могли прийти в любой банк страны и обменять свои бумажные деньги на эквивалент в золоте и обратно. Биткоин не обеспечен ничем, это чистая математика.

Фундаментальной частью биткойна являются криптографические алгоритмы. В частности, алгоритм ECDSA — Elliptic Curve Digital Signature Algorithm, который использует эллиптические кривые. В ECDSA для подписи и верификации используются разные процедуры, состоящие из нескольких арифметических операций.

Сокращенный вид уравнения эллиптической кривой выглядит так:

$$y^2 = x^3 + ax + b.$$

При a = 0 и b = 7 (версия, используемая биткоин) её вид представлен на рис. 2.:

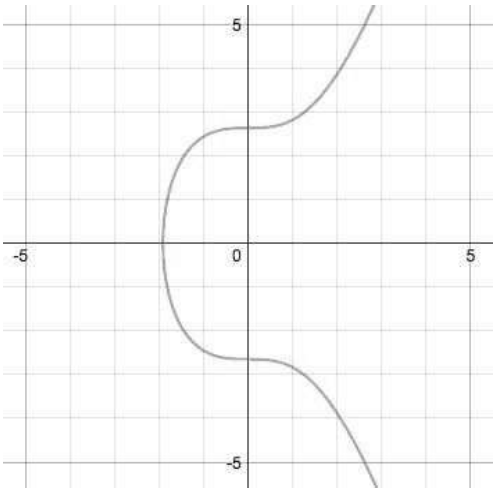

Рис. 2. Вид эллиптической кривой с параметрами a=0, b=7.

Эллиптические кривые имеют несколько интересных свойств, например, невертикальная линия PQ, пересекающая две некасательные точки на кривой (рис. 3), пересечет эллиптическую кривую в третьей точке (R`). Суммой двух точек на эллиптической кривой P + Q называется точка R, которая является отражением точки – R` (построенной путем продолжения прямой PQ до пересечения с кривой) относительно оси X. Точка P + Q = R определяется как отражение через ось X третьего пересечения R 'на прямой PQ (рис. 3).

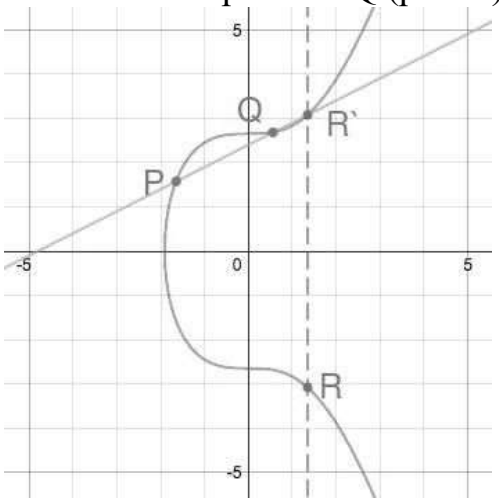

Рис. 3. Сумма двух точек на рассматриваемой эллиптичксой кривой.

Если мы хотим сложить точку саму с собой (удвоить её), то в этом случае просто проводится касательная в точке P. Полученная точка пересечения (R`) отражается симметрично относительно оси X (рис 4).

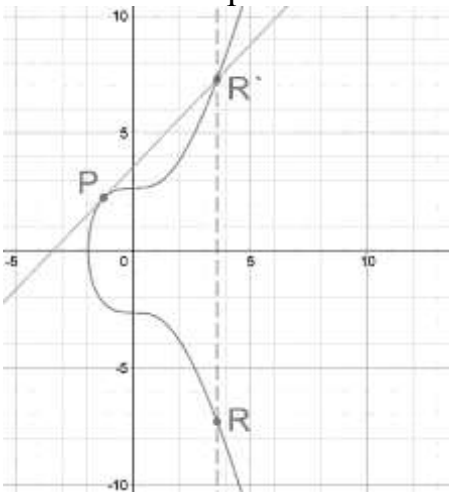

Рис. 4. Удвоение точки эллиптической кривой.

Как сложить точку саму с собой? Для этого определяется операция удвоения точки, P + P = R. При удвоении мы проводим прямую, касательную к данной эллиптической кривой в точке P, которая, согласно свойствам кривой, должна пересекать ее еще в одной точке R`. Точка R, симметричная R` относительно оси X, и будет считаться точкой удвоения P.

Эти две операции можно использовать, чтобы определить операцию скалярного умножения, R = a P, определяемую как добавление точки P самой к себе a раз. Например, R = 7P = P + (P + (P + (P + (P + (P + P))))). Процесс скалярного умножения, как правило, можно упростить, используя комбинацию сложения и удвоения точек. Например, R = 7P, R = P + 6P, R = P + 2 (3P) или R = P + 2 (P + 2P). Здесь операция 7P была разбита на два этапа удвоения точек и два сложения точек — в итоге, вместо 7 операций нужно произвести всего четыре.

И вот на этих математических операциях основано существование и функционирование сети биткоин. Чистая математика.

В заключение хотелось бы сказать, что в 2008 году, когда биткоин только появился, 1300 биткоинов стоили примерно 23 рубля. Первой реальной сделкой была покупка двух пицц стоимостью меньше 1000 рублей за 10000 биткоинов. В 2016 году один биткоин стоил 40000 рублей, а в конце 2017 года, только представьте, 1 биткоин стоил больше миллиона рублей. И не предел. По прогнозам некоторых аналитиков, к концу 2018 года 1 биткоин может стоить до 1000000 рублей. Таким образом, при отсутствии "ответственного центра" (или нескольких его инстанций) год электронная валюта Bitcoin развивается быстрыми темпами в довольно широких кругах людей, пользующихся высокой скоростью выполнения финансовых операций и их полной анонимностью. В связи с этим даже прогнозируется, что в ближайшие 10-15 лет криптовалюта может занять почетное место доллара США на мировом финансовом рынке! Однако многие финансисты все же считают, что традиционный доллар вряд ли возможно заменить цифровым эквивалентом в ближайшем будущем, потому как людям на данном этапе будет непросто отказаться от привычной банковской системы